STIC Search Report
EIC 2100

USPTO

STIC Database Tracking Number: 173616

TO:	From:
Cam-Linh T Nguyen **Location: RND 3C21** **Art Unit: 2161** **Wednesday, December 07, 2005** **Case Serial Number: 09/147869**	**Emory Damron** **Location: EIC 2100** **RND 4B19** **Phone: 571-272-3520** **Emory.Damron@uspto.gov**

Search Notes

Dear Cam-Linh,

Please find below your fast and focused results.
References of potential pertinence have been tagged, but please review all the packets in case you like something I didn't.
Of those references which have been tagged, please note any manual highlighting which I've done within the document.
In addition to searching on Dialog, I also searched EPO/JPO/Derwent and AltaVista.
There may be a few decent references contained herein, but I'll let you determine how useful they may be to you.
Please contact me if I can refocus or expand any aspect of this case, and please take a moment to provide any feedback (on the form provided) so EIC 2100 may better serve your needs. Good Luck!

Sincerely,
Emory Damron
Technical Information Specialist
EIC 2100, US Patent & Trademark Office
Phone: (571) 272-3520
Emory.damron@uspto.gov

sira
Search and Information Resources Administration

BEST AVAILABLE COPY F:F

Access DB# 173616

SEARCH REQUEST FORM

Scientific and Technical Information Center

Requester's Full Name: Nguyen, Cam Linh Examiner #: 78921 Date: 12/7/05
Art Unit: 2161 Phone Number ~~30~~ 2-4024 Serial Number: 09/471,869
Mail Box and Bldg/Room Location: RND - 3C21 Results Format Preferred (circle): PAPER DISK E-MAIL

If more than one search is submitted, please prioritize searches in order of need.

****

Please provide a detailed statement of the search topic, and describe as specifically as possible the subject matter to be searched. Include the elected species or structures, keywords, synonyms, acronyms, and registry numbers, and combine with the concept or utility of the invention. Define any terms that may have a special meaning. Give examples or relevant citations, authors, etc, if known. Please attach a copy of the cover sheet, pertinent claims, and abstract.

Title of Invention: Method & ~~Apparatus~~ for Managing information Related to Storage Activitie

Inventors (please provide full names): Phillips, Jeffrey ; Allen David ;
Serkez Brett ; Bouchard Peter

Earliest Priority Filing Date: 12/23/99

For Sequence Searches Only *Please include all pertinent information (parent, child, divisional, or issued patent numbers) along with the appropriate serial number.*

- plural of Backup Storage System (include : first, second & third system
- User interface
- Domain with back up systems
- Domain include first and second Back up storage systems & User interface
  but exclude the third back up storage system

EMC corp

X COPY

****

STAFF USE ONLY Type of Search Vendors and cost where applicable

Eunice DeRose

```
Set     Items   Description
S1    2274173   PLURAL? OR SEVERAL? OR MULTIPL? OR MULTIT? OR NUMEROUS? OR
            MANY OR MORE(2W)TWO
S2     999511   THREE? OR TRIO? OR TRIUNE? OR TRIAD? OR TRIPL? OR TERTIAR?
            OR THIRD OR 3RD
S3    3848717   FIRST? OR 1ST OR PRIMARY OR INITIAL? OR ORIGINAL? OR LEADO-
            FF? OR MAIN OR CHIEF OR INTRODUCTORY?
S4    3956269   SECOND? OR 2ND OR DOUBL? OR TWIN? OR EXTRA? OR DUPLICAT? OR
             ANOTHER OR SUBSIDIAR? OR AUXILIAR?
S5      50342   BACK?()UP OR BACKUP?
S6      39062   REDUNDAN? OR FAILSAFE? OR FAIL()SAFE?
S7     437875   RESERVE? OR SUPPLEMENTAL? OR SUPPLEMENTARY? OR EMERGENCY? -
            OR SUBSTITUT? OR SURROGAT?
S8    2657717   STORAG? OR STORE? OR STORING? OR MEMOR? OR CACHE? OR BUFFE-
            R? OR DOMAIN?
S9      29563   USER()INTERFACE? OR UI OR UIS OR GUI? ? OR (GRAPHIC? OR VI-
            SUAL?)(2W)INTERFACE?
S10     33082   MENU? ? OR DROPDOWN? OR DROP()DOWN? OR API? ? OR (APP OR A-
            PPS OR APPLICATION?)(2N)INTERFACE?
S11   2912921   EXCLUD? OR PREVENT?
S12   1543464   RESTRICT? OR DENY? OR DENIE? OR DENIAL? OR OBSTRUCT? OR BL-
            OCK? OR SHUTDOWN? OR SHUT?()DOWN
S13    429964   "NOT"()(ALLOW? OR ENABL? OR PERMIT?) OR DISALLOW? OR DISAB-
            L? OR SUSPEND? OR SUSPENSION?
S14    331407   AUTODISABL? OR NOGO OR NO()GO OR OFFSTATE? OR OFF()STATE? -
            OR INTERRUPT? OR TURNOFF? OR (TURN? OR SWITCH?)()OFF
S15    913901   STOP??? OR ARREST? OR IMPED? OR FORBID? OR HALT??? OR ABOR-
            T? OR SCRUB???? OR SCRATCH? OR NIX OR NIXES OR NIXED OR NIXING
S16   1267412   IC=G06F?
S17    962232   MC=T01?
S18       355   S1:S4 AND S5:S7 AND S8 AND S9:S10
S19        10   S18 AND S11:S15 AND S2
S20        71   S18 AND S16:S17 AND S11:S15
S21        75   S19:S20
S22    816090   PR=2000:2002
S23    815119   PR=2003:2005
S24        96   S18 AND S11:S15
S25        96   S21 OR S24
S26        66   S25 NOT S22:S23
S27        66   IDPAT (sorted in duplicate/non-duplicate order)
File 347:JAPIO Nov 1976-2005/Jul(Updated 051102)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200578
         (c) 2005  Thomson Derwent
```

27/3,K/28 (Item 28 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014685946 **Image available**
WPI Acc No: 2002-506650/200254
Related WPI Acc No: 2001-534717; 2002-050552; 2002-266023; 2002-442589; 2002-442590; 2003-090065; 2003-455900; 2004-153998; 2005-401619; 2005-589456
XRPX Acc No: N02-400826

Files copying method in personal computer, involves copying files identified in list of non-copied files to back - up **drive, to make** back - up **drive fully bootable drive**

Patent Assignee: ADAPTEC INC (ADAP-N)
Inventor: MAFFEZZONI G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6385707	B1	20020507	US 9875687	P	19980224	200254 B
			US 98110783	A	19980706	
			US 99256681	A	19990223	

Priority Applications (No Type Date): US 9875687 P 19980224; US 98110783 A 19980706; US 99256681 A 19990223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6385707	B1		42	G06F-011/20	Provisional application US 9875687 CIP of application US 98110783 CIP of patent US 6205527

... **method in personal computer, involves copying files identified in list of non-copied files to** back - up **drive, to make** back - up **drive fully bootable drive**

Abstract (Basic):

... an operating system during copying of selected files, is generated. The operating system is to **shut down** , to release the non-copied files. The files identified in the list of non-copied files, are copied to a **back - up** drive to make the **back - up** drive a fully bootable drive.

... 2) Computer-readable media **storing** program for copying locked system files...

...For copying files such as operating system files, program and data files from **primary** drive of a personal computer, to a **secondary** drive for intelligently **backing up** selected data from host computer's **main storage** drive...

... **Prevents** downtime productivity losses and assist the user in trouble shooting the failure, repairing the failure and restoring the failed system through a user friendly **graphical user interface** . Protects user's data and productivity upon experiencing a hard disk failure

International Patent Class (Main): **G06F-011/20**
Manual Codes (EPI/S-X): **T01-F05B** ...

... **T01-F05E** ...

... **T01-G03** ...

... **T01-H01C3** ...

... **T01-S03**

US006385707B1

(12) **United States Patent**
Maffezzoni

(10) **Patent No.: US 6,385,707 B1**
(45) **Date of Patent: May 7, 2002**

(54) **METHOD AND APPARATUS FOR BACKING UP A DISK DRIVE UPON A SYSTEM FAILURE**

(75) Inventor: **Guido Maffezzoni**, San Jose, CA (US)

(73) Assignee: **Adaptec, Inc.**, Milpitas, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/256,681**

(22) Filed: **Feb. 23, 1999**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/110,783, filed on Jul. 6, 1998, now Pat. No. 6,205,527.
(60) Provisional application No. 60/075,687, filed on Feb. 24, 1998.

(51) **Int. Cl.**[7] **G06F 11/20**
(52) **U.S. Cl.** **711/162**; 211/161; 211/163; 211/4; 211/111; 211/112; 211/113; 707/202; 707/203; 707/204; 714/13; 714/14; 714/15
(58) **Field of Search** 711/4, 111–114, 711/152, 161–163; 714/1–8, 13–15, 40–45; 707/202–204

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,819,159	A *	4/1989	Shipley et al.	714/15
5,269,022	A	12/1993	Shinjo et al.	713/2
5,469,573	A	11/1995	McGill, III et al.	713/1
5,546,534	A *	8/1996	Malcolm	714/6
5,615,364	A *	3/1997	Marks	707/202
5,675,725	A *	10/1997	Malcolm	714/6
5,694,600	A	12/1997	Khenson et al.	713/2
5,713,024	A	1/1998	Halladay	714/13
5,754,782	A	5/1998	Masada	709/219

OTHER PUBLICATIONS

Unknown, XactCopy Backup and Restore Strategy Promotional Materials and White Paper, DuoCor, Inc., Nevada City, CA (Jun. 1, 1998), 20 pages.

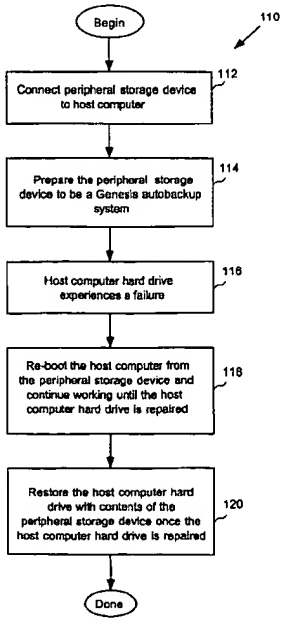
* cited by examiner

Primary Examiner—Than Nguyen
(74) *Attorney, Agent, or Firm*—Martine & Penilla, LLP

(57) **ABSTRACT**

A method and system for copying files between drives of a computer system is provided. The method begins where files are selected to be copied from a first drive of the computer system to a second drive of the computer system. The selected files include operating system files, program files and data files. The method then proceeds to commencing an initial copying of the selected files. While the initial files are being copied, a list of non-copied files is generated. The list of non-copied files represent files that are locked by an operating system. A raw data copy is performed during the initial copying by referencing a FAT table of the drive from which data is copied from for each file in the list of non-copied files. A shut down of the operating system is then commenced. The operating system is configured to shut down and release the files previously locked by the operating system. A driver is then implemented to cause a copying of the files identified in the list of non-copied files from the first drive to the second drive in order to make the second drive, which is receiving the files being copied, a reliable bootable drive. The method is also used to perform copying from the second drive to the first drive during a restoring operation.

20 Claims, 24 Drawing Sheets



In some embodiments, exemplary peripheral-type storage devices may include an extra hard drive(s), a digital video disk (DVD) drive, a CDRW drive, a CDR drive, a Magneto Optical Disk drive, etc. Furthermore, any type of host adapter can be used, regardless of whether it is integrated into a computer's motherboard or is integrated onto a host adapter card. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

What is claimed is:

1. A method for copying files from a primary drive of a computer system, comprising:

selecting files to be copied from the primary drive of the computer system to a backup drive, the selected files including operating system files and program and data files;

commencing an initial copying of the selected files;

generating a list of non-copied files during the copying of the selected files, the list of non-copied files represent files that are locked by an operating system running on the primary drive;

commencing a shut down of the operating system, the operating system being configured to shut down and release the files previously locked by the operating system; and

copying the files identified in the list of non-copied files from the primary drive to the backup drive in order to make the backup drive a fully bootable drive.

2. A method for copying files from a primary drive of a computer system as recited in claim **1**, wherein the list of non-copied files is temporarily stored in the system registry of the primary drive of the computer system.

3. A method for copying files from a primary drive of a computer system as recited in claim **1**, further comprising:

running a driver that is configured to be notified by the operating system that the shut down of the computer system has commenced; and

the driver being configured to refer to the system registry to find the list of non-copied files and trigger the copying of the files identified in the list of non-copied files from the primary drive to the backup drive.

4. A method for copying files from a primary drive of a computer system as recited in claim **3**, wherein the driver shuts down after the operating system, and the copying of the files identified in the list of non-copied files is performed after the operating system shuts down but before the driver shuts down.

5. A method for copying files from a primary drive of a computer system as recited in claim **3**, wherein the operating system is a Windows based operating system.

6. A method for copying files from a primary drive of a computer system as recited in claim **5**, wherein the Windows based operating system is an NT operating system.

7. A method for copying files from a primary drive of a computer system as recited in claim **1**, wherein the list of non-copied files are the operating system files.

8. A method for copying files from a primary drive of a computer system as recited in claim **1**, further comprising:

performing a raw data copy by referencing a FAT table of the primary drive for each file in the list of non-copied files while performing the initial copying of the selected files.

9. A system for copying locked system files from a first drive of a computer system to a second drive, comprising:

beginning a copying of selected files from the first drive to the second drive;

detecting one or more locked files while the copying of the selected files is in progress, the locked files are such that they are prevented from being copied from the first drive to the second drive;

generating a list of non-copied files that includes the one or more locked files, the generating being configured to occur while the copying of the selected files is in progress;

placing a path for the list of non-copied files in a system registry of the computer system;

beginning a shut down of the computer system, the shut down is configured to shut down an operating system of the computer system before software drivers are shut down; and

implementing a software driver to call on the list of non-copied files in the system registry, the software driver is further configured to cause a copying of the one or more locked files from the first drive to the second drive.

10. A system for copying locked system files from a first drive of a computer system to a second drive as recited in claim **9**, wherein an operating system running from the first drive locks system files that prevents the copying.

11. A system for copying locked system files from a first drive of a computer system to a second drive as recited in claim **10**, wherein when the operating system of the computer system shuts down, the one or more locked files are released by the operating system and made available for copying.

12. A system for copying locked system files from a first drive of a computer system to a second drive as recited in claim **10**, wherein the operating system is a Windows NT operating system.

13. A system for copying locked system files from a first drive of a computer system to a second drive as recited in claim **9**, wherein when the copying of the one or more locked files is complete, the second drive will be a bootable drive having a full set of system files.

14. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive, the computer readable media comprising:

program instructions for beginning a copying of selected files from the primary drive to the secondary drive;

program instructions for detecting one or more locked files while the copying of the selected files is in progress, the locked files are such that they are prevented from being copied from the primary drive to the secondary drive;

program instructions for generating a list on non-copied files that includes the one or more locked files, the generating being configured to occur while the copying of the selected files is in progress;

program instructions for placing a path for the list of non-copied files in a system registry of the computer system;

program instructions for beginning a shut down of the computer system, the shut down is configured to shut down an operating system of the computer system before software drivers are shut down; and

program instructions for implementing a software driver to call on the list of non-copied files in the system registry, the software drive further configured to cause

a copying of the one or more locked files from the primary drive to the secondary drive.

15. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive as recited in claim **14**, wherein an operating system running from the primary drive locked system files to prevent the copying.

16. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive as recited in claim **15**, wherein when the operating system of the computer system shuts down, the one or more locked files are released by the operating system and made available for copying.

17. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive as recited in claim **15**, wherein the operating system is a Windows NT operating system.

18. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive as recited in claim **14**, wherein when the copying of the one or more locked files is complete, the secondary drive will be a bootable drive having a full set of system files.

19. A computer readable media containing program instructions for copying locked system files from a primary drive of a computer system to a secondary drive as recited in claim **14**, further comprising:

program instructions for performing a raw data copy by referencing a FAT table of the primary drive for each file in the list of non-copied files while performing the copying of the selected files.

20. A method for copying files between drives of a computer system, comprising:

selecting files to be copied from a first drive of the computer system to a second drive of the computer system, the selected files including operating system files and program and data files;

commencing an initial copying of the selected files;

generating a list of non-copied files during the copying of the selected files, the list of non-copied files represent files that are locked by an operating system;

performing a raw data copy by referencing a FAT table of the drive from which data is copied for each file in the list of non-copied files while performing the initial copying of the selected files;

commencing a shut down of the operating system, the operating system being configured to shut down and release the files previously locked by the operating system; and

implementing a driver to cause a copying of the files identified in the list of non-copied files from the first drive to the second drive in order to make the second drive, which is receiving the files being copied, a fully bootable drive.

* * * * *

27/3,K/54 (Item 54 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009100438 **Image available**
WPI Acc No: 1992-227868/199228
Related WPI Acc No: 1997-297637
XRPX Acc No: N92-173260
Data-loss prevention **software product for DOS computer - has continuous on-line, real-time** back - up **by replicating drive read-write activity to** primary **or** secondary **drives**
Patent Assignee: NONSTOP NETWORKS LTD (NONS-N)
Inventor: CARD S; CLOWES R F; TIMS F W; TIMS J F
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2251502	A	19920708	GB 9123339	A	19911104	199228	B
GB 2251502	B	19950614	GB 9123339	A	19911104	199527	

Priority Applications (No Type Date): US 90610181 A 19901107
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2251502	A		77	G06F-011/16	
GB 2251502	B		3	G06F-011/16	

Data-loss prevention **software product for DOS computer...**
...has continuous on-line, real-time back - up **by replicating drive read-write activity to** primary **or** secondary **drives**

...Abstract (Basic): comprises executable code which includes: command system to load the executable code into workstation RAM; **user interface** enabling a user to specify one drive as a **primary** logical drive to be replicated; system request filter to examine system requests generated by the application and intercept a **primary** logical drive request before it is processed by the drive sub-system; and drive-request processor to replicate and issue the **first** drive request to a user-specified **secondary** of the logical drives before issuing a succeeding drive-request to the **primary** drive...

...A processor processes a succeeding drive request in a similar manner to the **first** drive request after issuing the **first** drive request to the **secondary** drive. The system maintains a functionally identical mirrored data image on the **secondary** drive of the data activity issued to the **primary** drive by the **primary** drive requests, without user intervention...
...Abstract (Equivalent): A fault-tolerant computer network comprising: a) at least a **primary** and a **secondary** file server; b) a **primary** server-supported network data **storage** system maintaining a **primary** data image and a **secondary** data **storage** system supported by said **secondary** file server; c) a **plurality** of personal computer workstations networked with said **primary** server, each said workstation being an intelligent data-processing work station booted with an operating system; and d) data-access software implemented in random access **memory** at each work station which data access software performs the steps of: i) monitoring all **primary** -destined data-change-related requests output by the respective workstation and routed to said **primary** data **storage** system; and ii) after receipt of each **primary** -destined data-change-related request by the **primary** server, redirecting the request to the **secondary** data- **storage** system before issuing a succeeding data-change-related-request to the **primary** data **storage** system; thereby to automatically and

continually maintain a functionally identical mirrored data image on said **secondary** data **storage** system of the data-change-related activity at said **primary** data **storage** system without user intervention; iii) detecting at the workstation loss of access to said **primary** data **storage** system via said **primary** server; iv) rerouting workstation-generated data **storage** activity intended for said **primary** data **storage** system to said **secondary** data **storage** system in response to loss of access to said **primary** data **storage** system via said **primary** server; and v) prior to loss of data access via the **primary** server, suppressing data-change related request for said **secondary** server by users routing requests thereto specifying said **secondary** data **storage** system; whereby the workstation, in operations proceeding transparently to the user, can access said functionally identical mirrored data image on said **secondary** data **storage** system after loss of data access to said **primary** data **storage** system...

...Title Terms: **PREVENT** ;

International Patent Class (Main): **G06F-011/16**

Manual Codes (EPI/S-X): **T01-G03** ...

... **T01-G05B** ...

... **T01-H01C**

(12) UK Patent Application (19) GB (11) 2 251 502 (13) A

(43) Date of A publication 08.07.1992

(21) Application No 0123339.5

(22) Date of filing 04.11.1991

(30) Priority data
(31) 07610181 (32) 07.11.1990 (33) US

(71) Applicant
Nonstop Networks Limited

(Incorporated in the USA – New York)

20 Waterside, New York, NY 10010,
United States of America

(72) Inventors
Fred William Tims
James Frank Tims
Stuart Card
Richard French Clowes

(74) Agent and/or Address for Service
Marian Crawford Clarke
Lythwood, Bayston Hill, Shrewsbury, SY3 0AU,
United Kingdom

(51) INT CL[5]
G06F 11/16

(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
EP 0221275 A2 US 4488223 A

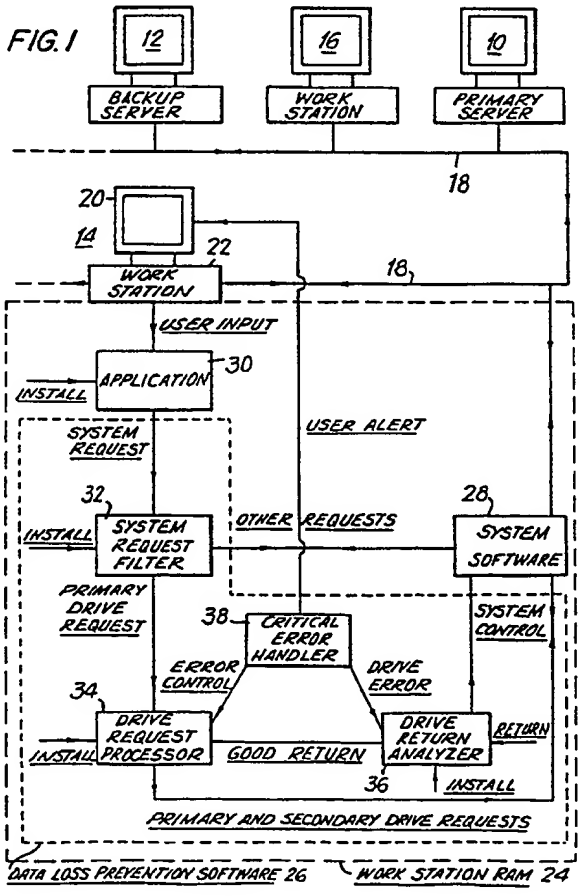
(58) Field of search
UK CL (Edition K) G4A AAP AEX
INT CL[5] G06F 11/00 11/16 11/20 12/16
Online database: WPI

(54) Data-loss prevention

(57) This invention provides: a data-loss prevention software product; methods of preventing data loss; and personal computer systems and networks using said data-loss prevention product. Preferred embodiments provide DOS computer systems, especially networked, with continuous, on-line, real-time back-up by way of replication of all drive read/write activity to a primary and one or more secondary logical drives. Users are alerted to drive failure and user-confirmed automatic continuation of processing or non-stop processing, on a secondary drive is also provided.

"ONE OR MORE SECONDARY DRIVES", CLAIM 10

FIG. 1



GB 2 251 502 A

CLAIMS

1. A data-loss prevention software product for an intelligent personal-computer workstation which workstation is connected to a plurality of logical drives for data storage each of which logical drives is a random-access storage device or a sub-division thereof, and which workstation has data-entry means for a user to input data to the workstation and has random-access-main-memory areas (RAM) capable of supporting system software and an application to receive data-entry instructions from said data-entry means and generate data-related drive requests, which application can include a system software user-interface , wherein the software product comprises executable code which includes:

a) command means to load the executable code into workstation RAM;

b) user interface means enabling a user to specify one of said drives as a primary logical drive to be replicated;

c) system request filter means to examine system requests generated by the application and intercept a primary logical drive request before it is processed by the drive sub-system;

d) drive-request processor means to replicate and issue the first drive request to a user-specified secondary of said logical drives before issuing a succeeding

drive-request to the primary drive; and

e) means to process a succeeding drive request in a similar manner to said first drive request after issuing said first drive request to said secondary drive;

thereby to be capable of automatically and continually maintaining a functionally identical mirrored data image on said secondary drive of the data activity issued to the primary drive by said primary drive requests, without user intervention.

2. A software product according to claim 1 wherein all primary drive requests are processed as recited therein, thereby to be capable of maintaining a complete data image of said primary drive on said secondary drive.

3. A software product according to claim 1 which also includes:

drive-return analyzer means to examine returns from said logical drives; and

error-handling means which includes user-alerting means;

whereby a good drive return permits the issuance of the next succeeding drive request and a return signifying an unrecoverable disk error activates said user-alerting means.

4. A software product according to claim 3 wherein said system request filter means intercepts both primary drive reads

and primary drive writes and drive read returns are examined by the drive-return analyzer.

5. A software product according to claim 1 for a DOS computer wherein said software product and workstation are respectively capable of running under and running Microsoft Corporation's MS-DOS v. 3.1 or higher, or IBM Corporation's PC-DOS v. 3.1 or higher, or functional equivalents of either.

6. A software product according to claim 5 wherein said system request filter means uses a DOS interrupt to intercept primary drive requests.

7. A software product according to claim 1 comprising automatic means to continue processing data in the event of a failure of the primary drive which automatic means comprises: means to generate a user alert; and means to switch processing to said secondary drive using the functionally identical data image replicated thereon.

8. A software product according to claim 7 wherein said automatic means to continue processing comprises a critical error handler to suspend processing and take over system control.

9. A software product according to claim 8 wherein the critical error handler can act to instruct the drive request

processor to direct drive requests solely to a surviving drive or drives.

10. A software product according to claim 9 including means to permit a user to elect to discontinue processing in the event of drive failure wherein the critical error handler includes routines to close open files and exit gracefully.

11. A software product according to claim 10 characterized by being capable of occupying less than 30 KB of RAM when loaded in normal main memory and of reducing workstation application-processing performance by no more than 10%.

12. A software product according to claim 1 adapted to provide data replication to multiple secondary drives.

13. A software product according to claim 1 supplied on a transportable drive medium and packaged with a hard copy of detailed instructions for the installation and use of said software product.

14. An intelligent personal computer workstation which comprises:

a) data-entry means for a user to input data to the workstation;

b) random-access-main-memory areas (RAM) capable of

supporting system software and an application;

c) said data-entry means being usable to input data-changing activity to said application, wherein the workstation is connected to a plurality of logical drives for data storage each of which logical drives is a random-access storage device or a sub-division thereof, in combination with a data-loss prevention software product comprising executable code which includes:

d) command means to load the executable code into workstation RAM;

e) user interface means enabling a user to specify one of said drives as a primary logical drive to be replicated;

f) system request filter means to examine system requests generated by said application and intercept a first primary logical drive request;

g) drive-request processor means to replicate and issue the first drive request to a user-specified secondary of said logical drives before issuing a succeeding drive-request to the primary drive; and

h) means to process a succeeding drive request in a similar manner to said first drive request after issuing said first drive request to said secondary drive;

thereby to be capable of automatically and continually

maintaining a functionally identical mirrored data image on said secondary drive of the data activity issued to the primary drive by said primary drive requests, without user intervention.

15. A workstation according to claim 14 which is a DOS computer wherein said software product and workstation are respectively capable of running under and running Microsoft Corporation's MS-DOS v. 3.1 or higher, or IBM Corporation's PC-DOS v. 3.1 or higher, or functional equivalents of either.

16. A workstation according to claim 14 wherein the software product includes automatic means to continue processing data in the event of a failure of the primary drive which automatic means comprises: means to generate a user alert; and means to switch processing to said secondary drive using the functionally identical data image replicated thereon.

17. A workstation according to claim 16 wherein the critical error handler can act to instruct the drive request processor to direct drive requests solely to a surviving drive or drives.

18. A computer network comprising an interconnected file server and a workstation-and-software product as set forth in claim 14 wherein said primary logical drive is located on the file server.

19. A network according to claim 18 comprising a plurality of such workstations and associated software product, wherein each of said workstations can be installed to use the same logical drive on the file server as its primary logical drive.

20. A network according to claim 19 further comprising at least one backup file server connected to the workstations wherein the workstations can each use the same logical drive on the backup file server as their secondary drive.

21. A personal computer network comprising a primary file server having a primary logical drive for data storage, a backup file server having a secondary logical drive for data storage each of which logical drives is a random-access storage device or a sub-division thereof, and comprising a plurality of intelligent personal computer work stations connected to each said file server wherein each of said work stations includes:

a) data-entry means for a user to input data to said workstation; and

b) random-access-main-memory areas (RAM) capable of supporting system software and an application, said data-entry means being usable to input data-changing activity to said application;

in combination with a data-loss prevention software product at each workstation which product comprises executable code which code includes:

c) command means to load the executable code into workstation RAM;

d) system request filter means to examine system requests generated by said application and intercept a first primary logical drive request;

e) drive-request processor means to replicate and issue the first drive request to a user-specified secondary of said logical drives before issuing a succeeding drive-request to the primary drive; and

f) means to process a succeeding drive request in a similar manner to said first drive request after issuing said first drive request to said secondary drive;

thereby to be capable of automatically and continually maintaining a functionally identical mirrored data image on said secondary drive of the data activity issued to the primary drive by said primary drive requests, without user intervention.

22. A computer network according to claim 21 wherein the software product includes automatic means to continue processing data in the event of a failure of the primary drive which automatic means comprises: means to generate a user alert; and means to switch processing to said secondary drive using the functionally identical data image replicated thereon.

23. A method of preventing data loss on an intelligent

personal computer workstation which method includes the steps of:

a) sequentially inputting first then second data then subsequent data segments;

b) generating a first drive request for storage of said first data segment on a primary logical drive being a random-access storage device or a sub-division thereof;

c) intercepting said first drive request;

d) replicating and sending said intercepted first drive request to said primary logical drive;

e) relabeling and sending the replicated first drive request to a secondary logical drive for storage thereon, said secondary logical drive also being a random-access storage device or a sub-division thereof;

f) subsequently to said sending of said replicated first drive request to said secondary logical drive, generating a second drive request for storage of said second data segment on said primary logical drive;

g) processing said second drive request in the same manner as the first drive request; and

h) repeating the drive-request processing for subsequent data segments;

thereby to produce a functionally identical data image on said secondary logical drive of the data on said primary logical drive.

24. A method according to claim 23 for preventing data loss

on a DOS computer wherein said data-loss-prevention steps are carried out in RAM under DOS, which DOS is Microsoft Corporation's MS-DOS v. 3.1 or higher, or IBM Corporation's PC-DOS v. 3.1 or higher, or functional equivalents of either.

27/3,K/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015996148 **Image available**
WPI Acc No: 2004-153998/200415
Related WPI Acc No: 2001-534717; 2002-050552; 2002-266023; 2002-442589; 2002-442590; 2002-506650; 2003-090065; 2003-455900; 2005-401619; 2005-589456
XRPX Acc No: N04-123033

Database generating method for backup **system, involves defining** backup **set of data associated with booting operation of operating system available in** primary storage **device to be copied hard drive/removable media drive**

Patent Assignee: ADAPTEC INC (ADAP-N)
Inventor: GOSHEY M M; LUONG K N
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6684229	B1	20040127	US 9875687	P	19980224	200415 B
			US 98110783	A	19980706	
			US 99256676	A	19990223	

Priority Applications (No Type Date): US 9875687 P 19980224; US 98110783 A 19980706; US 99256676 A 19990223
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6684229	B1		42	G06F-017/30	Provisional application US 9875687 CIP of application US 98110783 CIP of patent US 6205527

Database generating method for backup **system, involves defining** backup **set of data associated with booting operation of operating system available in** primary storage **device to be copied hard drive/removable media drive**

Abstract (Basic):
... A **graphical user interface** (**GUI**) to display the information from a database is generated. An user defines a **backup** set of data associated with booting operation of an operating system that is available in a **primary storage** device to be copied to hard drive/removable media drive, as graphic object of the **GUI** proximate to each item of displayed information.
... An INDEPENDENT CLAIM is also included for computer readable medium **storing** database generating program...

...For generating database of data resident on **primary storage** device of computer system used in **backup** system...
...data is copied to the hard drive/removable media drive, loss of the data is **prevented** . The tremendous downtime is eliminated when hard disk crash is experienced. The user productivity no...
...Title Terms: **PRIMARY** ;
International Patent Class (Main): **G06F-017/30**
Manual Codes (EPI/S-X): **T01-F05B2** ...

... **T01-J05B4M** ...

... **T01-S03**

US006684229B1

(12) **United States Patent**
Luong et al.

(10) **Patent No.: US 6,684,229 B1**
(45) **Date of Patent: Jan. 27, 2004**

(54) **METHOD OF GENERATING A DATABASE FOR USE IN AN INTELLIGENT BACKUP AND RESTORING SYSTEM**

(75) Inventors: **Kristine N. Luong**, Santa Clara, CA (US); **Michael M. Goshey**, San Jose, CA (US)

(73) Assignee: **Adaptec, Inc.**, Milpitas, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/256,676**

(22) Filed: **Feb. 23, 1999**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/110,783, filed on Jul. 6, 1998, now Pat. No. 6,205,527.
(60) Provisional application No. 60/075,687, filed on Feb. 24, 1998.

(51) **Int. Cl.**[7] **G06F 17/30**
(52) **U.S. Cl.** **707/204**; 707/102; 707/201; 707/202; 711/162
(58) **Field of Search** 707/204, 203, 707/202, 201; 711/162; 345/334, 356, 162

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,079,740	A *	1/1992	Patel et al.	714/10
5,269,022	A	12/1993	Shinjo et al.	395/700
5,469,573	A	11/1995	McGill, III et al.	395/700
5,638,509	A *	6/1997	Dunphy et al.	714/20
5,694,600	A	12/1997	Khenson et al.	395/652
5,708,776	A *	1/1998	Kikinis	714/55
5,713,024	A *	1/1998	Halladay	395/712
5,754,782	A	5/1998	Masada	395/200.43
5,761,677	A *	6/1998	Senator et al.	707/203
5,873,101	A *	2/1999	Klein	707/204
5,884,324	A *	3/1999	Cheng et al.	707/201
6,205,527	B1 *	3/2001	Goshey et al.	711/162
6,324,654	B1 *	11/2001	Wahl et al.	714/6
6,446,090	B1 *	9/2002	Hart	707/201
6,477,629	B1 *	11/2002	Goshey et al.	711/162
2003/0167419	A1 *	9/2003	Yanai et al.	714/7

OTHER PUBLICATIONS

Unknown, *XactCopy Backup and Restore Strategy Promotional Materials and White Paper*, DuoCor, Inc., Nevada City, CA (Jun. 1, 1998), 20 pages.

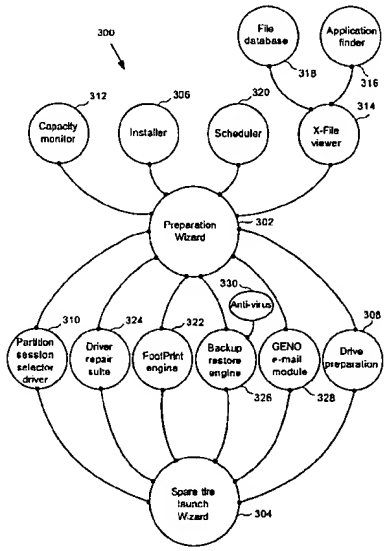
* cited by examiner

Primary Examiner—Jean R. Homere
(74) *Attorney, Agent, or Firm*—Martine & Penilla, LLP

(57) **ABSTRACT**

A method for generating a database of data resident on a primary storage device of a computer system for use in a backup system associated with the computer system includes generating a database having information associated with data resident on the primary storage device of the computer system. A graphical user interface is then generated to display the information in the database. The displayed information is preferably configured to be selected by a user to define a backup set of data that is available to be copied from the primary storage device of the computer system to a secondary storage device connected to the computer system. The method may further include the operations of setting a flag to designate selected portions of the database, and writing the selected portions of the database to the primary storage device of the computer system. A computer readable media for generating a database of data resident on a primary storage device of a computer system for use in a backup system associated with the computer system also is described.

23 Claims, 24 Drawing Sheets



medium and be loaded or installed onto the computer system **800** when needed. Removable program mediums include, for example, CD-ROM, PC-CARD, floppy disk, and magnetic tape.

The network interface **812** is used to send and receive data over a network connected to other computer systems. An interface card or similar device and appropriate software implemented by the microprocessor **816** can be used to connect the computer system **800** to an existing network and transfer data according to standard protocols.

The keyboard **814** is used by a user to input commands and other instructions to the computer system **800**. Other types of user input devices can also be used in conjunction with the present invention. For example, pointing devices such as a computer mouse, a track ball, a stylus, or a tablet can be used to manipulate a pointer on a screen of a general purpose computer.

The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data that can be thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random access memory, CD-ROMs, magnetic tape, and optical data storage devices. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For example, although a preferred type of peripheral storage device is a Jaz™ drive, any type of peripheral storage devices or built-in computer storage devices can be used. In addition, the storage devices can be either physically located next to the computer system itself or remotely networked over, e.g., a local area network (LAN) or the Internet.

In some embodiments, exemplary peripheral-type storage devices may include an extra hard drive(s), a digital video disk (DVD) drive, a CDRW drive, a CDR drive, a Magneto Optical Disk drive, etc. Furthermore, any type of host adapter can be used, regardless of whether it is integrated into a computer's motherboard or is integrated onto a host adapter card. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

What is claimed is:

1. A method for generating a database of data resident on a primary storage device of a computer system for use in a backup system associated with the computer system, comprising:

generating a database having information associated with data resident on the primary storage device of the computer system; and

generating a graphical user interface to display the information in the database, the graphical user interface including a graphic object proximate to each item of displayed information to enable a user to define a backup set of data that is available to be copied from the primary storage device of the computer system to a secondary storage device connected to the computer system, the backup set of data automatically including information associated with an operating system and information required for booting the operating system.

2. The method of claim **1**, further comprising:

setting a flag to designate selected portions of the database; and

writing the selected portions of the database to the primary storage device of the computer system.

3. The method of claim **1**, wherein the information associated with data resident on the primary storage device includes a list of programs installed on the primary storage device and a list of logical hard drives together with all files on the logical hard drives.

4. The method of claim **3**, wherein the graphical user interface is configured to display a first view including the list of programs installed on the primary storage device and a second view including the list of logical hard drives together with the files on the logical hard drives.

5. The method of claim **4**, wherein the graphical user interface includes a capacity monitor that displays the disk space occupied by selected portions of the database.

6. The method of claim **1**, wherein the graphical user interface is configured to display a dialog box including a first radio button that selects a minimal backup set of data and a second radio button that selects a maximal backup set of data.

7. The method of claim **6**, wherein the minimal backup set of data includes the information associated with the operating system and the information required for booting the operating system and the maximal backup set of data includes all files on the primary storage device.

8. The method of claim **1**, wherein the secondary storage device is one of a hard drive and a removable media drive.

9. The method of claim **1**, wherein the computer system is a personal computer.

10. A method for generating a database of programs and files resident on a primary storage device of a computer system for use in a backup system associated with the computer system, comprising:

generating a database of programs installed on the primary storage device of the computer system and files resident on the primary storage device of the computer system; and

generating a graphical user interface to display the programs and files in the database, the graphical user interface being configured to display a first view including the programs and a second view including the files, the programs and files being displayed for selection by a user to define a backup set of data that is available to be copied from the primary storage device of the computer system to a secondary storage device connected to the computer system, the backup set of data automatically including information associated with an operating system and information required for booting the operating system.

11. The method of claim **10**, further comprising:

setting a flag to designate selected programs and files; and

writing the selected programs and files to the primary storage device of the computer system.

12. The method of claim **10**, wherein the second view includes a list of logical hard drives together with the files on the logical hard drives.

13. The method of claim **10**, wherein the graphical user interface is configured to display a dialog box including a first radio button that selects a minimal backup set of data and a second radio button that selects a maximal backup set of data.

14. The method of claim **13**, wherein the minimal backup set of data includes the information associated with the

operating system and the information required for booting the operating system and the maximal backup set of data includes all files on the primary storage device.

15. The method of claim **1**, wherein the secondary storage device is one of a hard drive and a removable media drive.

16. The method of claim **1**, wherein the computer system is a personal computer.

17. A computer readable media containing program instructions for generating a database of data resident on a primary storage device of a computer system for use in a backup system associated with the computer system, the computer readable media comprising:

program instructions for generating a database having information associated with data resident on a primary storage device of the computer system; and

program instructions for generating a graphical user interface to display the information in the database, the graphical user interface including a graphic object proximate to each item of displayed information to enable a user to define a backup set of data that is available to be copied from the primary storage device of the computer system to a secondary storage device connected to the computer system, the backup set of data automatically including information associated with an operating system and information required for booting the operating system.

18. The computer readable media of claim **17**, further comprising:

program instructions for setting a flag to designate selected portions of the database; and

program instructions for writing the selected portions of the database to the primary storage device of the computer system.

19. The computer readable media of claim **17**, wherein the information associated with data resident on the primary storage device includes a list of programs installed on the primary storage device and a list of logical hard drives together with all files on the logical hard drives.

20. The computer readable media of claim **19**, wherein the graphical user interface is configured to display a first view including the list of programs installed on the primary storage device and a second view including the list of logical hard drives together with the files on the logical hard drives.

21. The computer readable media of claim **17**, wherein the graphical user interface includes a capacity monitor that displays the disk space occupied by selected portions of the database.

22. The computer readable media of claim **17**, wherein the graphical user interface is configured to display a dialog box including a first radio button that selects a minimal backup set of data and a second radio button that selects a maximal backup set of data.

23. The computer readable media of claim **22**, wherein the minimal backup set of data includes the information associated with the operating system and the information required for booting the operating system and the maximal backup set of data includes all files on the primary storage device.

* * * * *

27/3,K/45 (Item 45 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012598583 **Image available**
WPI Acc No: 1999-404689/199934
XRPX Acc No: N99-301657
Critical files management method for information handling system
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: PERKS M A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5924102	A	19990713	US 97852777	A	19970507	199934	B

Priority Applications (No Type Date): US 97852777 A 19970507
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5924102	A		9	G06F-017/30	

Abstract (Basic):
... A **memory stores** the instructions and data for usage by the processors. The programs (52) registers and unregisters the critical files in a critical file manager (50) through an **application** programming **interface** (**API**) (56). When a user modifies a critical file, the program notices the manager about the...
... An input-output unit communicates the information between the peripherals and **several** processors. When the critical file is modified, a **backup** of the file is produced by the manager. When a **restriction** to modify a critical file is specified, security measures are implemented to prohibit modification of...

...Critical files are easily maintained and **backed - up** without requiring large amount of time or system resources. Critical files are easily and quickly...

...The figure shows **block** diagram of critical file management system...

... **API** (**Application** programming **interface**) (56
International Patent Class (Main): **G06F-017/30**
Manual Codes (EPI/S-X): **T01-J05B**

US005924102A

United States Patent [19]

Perks

[11] Patent Number: 5,924,102

[45] Date of Patent: Jul. 13, 1999

[54] **SYSTEM AND METHOD FOR MANAGING CRITICAL FILES**

[75] Inventor: **Michael Albert Perks**, Austin, Tex.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **08/852,777**

[22] Filed: **May 7, 1997**

[51] **Int. Cl.**[6] **G06F 17/30**

[52] **U.S. Cl.** **707/200**

[58] **Field of Search** 707/200

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,313,646	5/1994	Hendricks et al.	707/101
5,448,045	9/1995	Clark	235/382
5,471,615	11/1995	Amatsu et al.	395/200.32
5,638,509	6/1997	Dunphy et al.	395/182.18

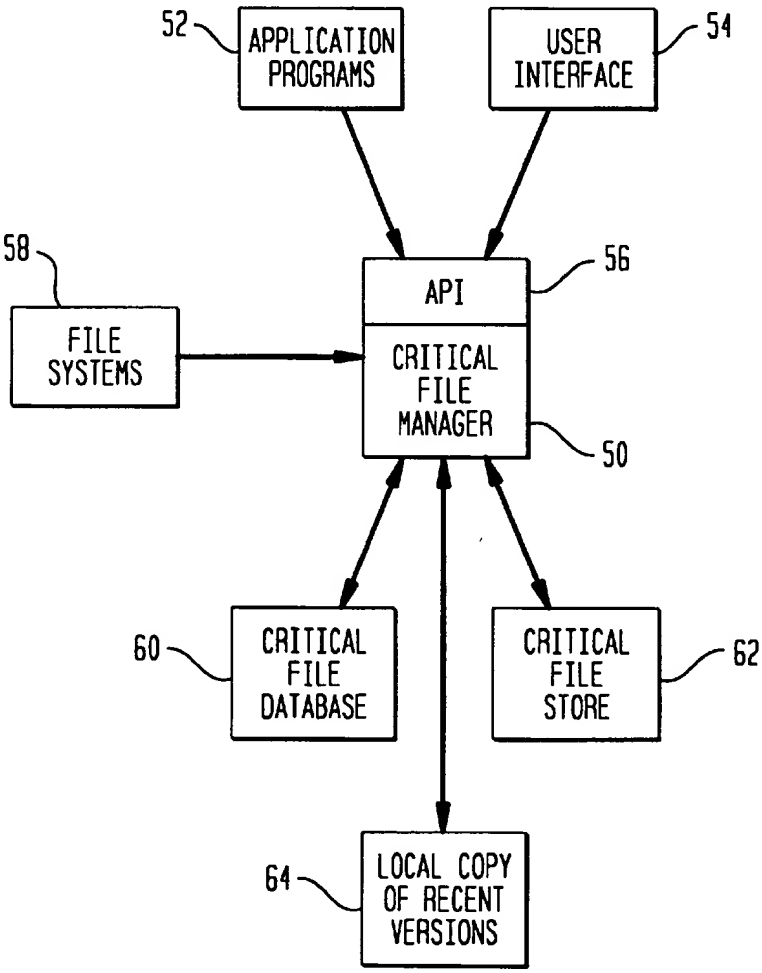
Primary Examiner—Maria N. Von Buhr

Attorney, Agent, or Firm—Leslie A.Van Leeuwen

[57] **ABSTRACT**

A system and method for managing critical files in an information handling system. Critical files are those files which are difficult to recover after a system failure, hard disk reformat, or user error. The critical file management system of the present invention includes a critical file manager, which can be accessed by programs through an application programming interface (API). Programs call the API to register and unregister critical files. A user interface is also provided. The user interface allows users to register and unregister critical files, and also allows users to view a list of all critical files and versions, along with the name of the program or user which added each critical file to the list. Users may also request a backup or restore of one, several, or all critical files at any time. A database of critical files, including a version for each file, is maintained. Backup copies of each critical file are stored in a critical file storage. At predetermined times, such as system shutdown or boot, the critical files are backed up. The critical file management system may also automatically restore all critical files at predetermined times, such as every time the information handling system is started.

24 Claims, 4 Drawing Sheets



When a user modifies a critical file (step **92**), the information handling system's file system notifies CFM **50** that a critical file has been changed (step **94**). CFM **50** then marks the file in critical file database **60** as a file requiring backup (step **96**). If a user modifies a critical file while working within an application program (steps **98** and **100**), the application program uses API **56** to notify CFM **50** that a critical file has been changed (step **102**). CFM **50** then marks the file in critical file database **60** as a file requiring backup (step **104**). As discussed above, security measures may be added to the system to prevent a user from modifying a particular file or files.

A user may use user interface **54** to request that a file be added to critical file database **60** (step **106**). In this case, CFM **50** adds the file to critical file database **60** (step **108**). Similarly, a user may use user interface **54** to request that a file be deleted from critical file database **60** (step **110**). In this case, CFM **50** deletes the file from critical file database **60** (step **112**).

At certain times, CFM **50** will backup critical files. For example, when a user shuts down or reboots the system (step **114**), CFM **50** determines if any critical files have been marked as requiring modification (step **116**). If so, CFM **50** will ask the user whether or not a critical file backup should be performed. If the user requests a critical file backup at this time (step **118**), CFM **50** stores any modified critical files in critical file store **62** (step **120**). Also, if the user has requested that the most recent copy of each critical file be stored in local copy **64**, CFM **50** will also copy the newest version of critical files to local copy **64**.

The user may also request a critical file backup at any time (step **122**), and CFM **50** will perform the backup (step **124**). Also, the user may request a critical file restore at any time (step **126**), and CFM **50** will restore each selected critical file from critical file store **62** (step **128**), or from local copy **64**. Note that in step **126** a user may request that one, several, or all critical files be restored.

Although the invention has been described with a certain degree of particularity, it should be recognized that elements thereof may be altered by persons skilled in the art without departing from the spirit and scope of the invention. One of the embodiments of the invention can be implemented as sets of instructions resident in the random access memory **16** of one or more computer systems configured generally as described in FIG. **1**. Until required by the computer system, the set of instructions may be stored in another computer readable memory, for example in a hard disk drive, or in a removable memory such as an optical disk for eventual use in a CD-ROM drive or a floppy disk for eventual use in a floppy disk drive. Further, the set of instructions can be stored in the memory of another computer and transmitted over a local area network or a wide area network, such as the Internet, when desired by the user. One skilled in the art would appreciate that the physical storage of the sets of instructions physically changes the medium upon which it is stored electrically, magnetically, or chemically so that the medium carries computer readable information. The invention is limited only by the following claims and their equivalents.

What is claimed is:

1. An information handling system comprising:

one or more processors;

input/output means for communicating information to and from one or more peripheral devices;

memory means for storing instructions and data for use by said processors;

one or more images of an operating system for controlling the operation of said processors;

at least one system bus connecting the elements of the system for efficient operation;

one or more programs executing in said processors; and

a critical file management system, comprising:

a critical file manager;

means for storing one or more critical files in a critical file storage memory means;

means for each program to identify one or more program files as critical files to said critical file manager; and

means for each program to notify said critical file manager whenever one or more of the program files identified as critical files is modified.

2. An information handling system according to claim **1**, further comprising means for each program to delete one or more of the program files identified as critical files from said critical file management system.

3. An information handling system according to claim **1**, further comprising means for maintaining a list of all critical files.

4. An information handling system according to claim **3**, wherein said means for maintaining a list of all critical files comprises a critical file database.

5. An information handling system according to claim **1**, further comprising means for backing up one or more critical files.

6. An information handling system according to claim **1**, further comprising means for restoring one or more critical files.

7. A critical file management system comprising:

a critical file manager;

means for storing one or more critical files in a critical file storage memory means;

means for a program to identify one or more program files as critical files to said critical file manager; and

means for the program to notify said critical file manager whenever one or more of the program files identified as critical files is modified.

8. A critical file management system according to claim **7**, further comprising means for the program to delete one or more of the program files identified as critical files from said critical file management system.

9. A critical file management system according to claim **9**, further comprising means for maintaining a list of all critical files.

10. A critical file management system according to claim **9**, wherein said means for maintaining a list of all critical files comprises a critical file database.

11. A critical file management system according to claim **7**, further comprising means for backing up one or more critical files.

12. A critical file management system according to claim **7**, further comprising means for restoring one or more critical files.

13. A method for managing critical files in an information handling system, comprising the steps of:

storing one or more critical files in a critical file storage memory means;

identifying, by a program executing in the information handling system, one or more program files as critical files to a critical file manager;

notifying, by the program, the critical file manager whenever one or more of the program files identified as critical files is modified.

14. A method according to claim **13**, further comprising the step of deleting, by the program, one or more of the

program files identified as critical files from said critical file management system.

15. A method according to claim **13**, further comprising the step of maintaining a list of all critical files.

16. A method according to claim **15**, wherein said maintaining step comprises storing the list of critical files in a critical file database.

17. A method according to claim **13**, further comprising the step of backing up one or more critical files.

18. A method according to claim **13**, further comprising the step of restoring one or more critical files.

19. A computer-readable medium for managing critical files in an information handling system, comprising:

a critical file manager;

means for storing one or more critical files in a critical file storage memory means;

means for a program executing in the information handling system to identify one or more program files as critical files to said critical file manager; and

means for the program to notify said critical file manager whenever one or more of the program files identified as critical files is modified.

20. A computer-readable medium according to claim **19**, further comprising means for the program to delete one or more of the program files identified as critical files from said critical file management system.

21. A computer-readable medium according to claim **19**, further comprising means for maintaining a list of all critical files.

22. A computer-readable medium according to claim **21**, wherein said means for maintaining a list of all critical files comprises a critical file database.

23. A computer-readable medium according to claim **19**, further comprising means for backing up one or more critical files.

24. A computer-readable medium according to claim **19**, further comprising means for restoring one or more critical files.

* * * * *

US006205527B1

(12) **United States Patent**
Goshey et al.

(10) **Patent No.: US 6,205,527 B1**
(45) **Date of Patent: Mar. 20, 2001**

(54) **INTELLIGENT BACKUP AND RESTORING SYSTEM AND METHOD FOR IMPLEMENTING THE SAME**

(75) Inventors: **Michael M. Goshey**; **Guido Maffezzoni**; **Gilbert Chang-Tying Wu**, all of San Jose; **Yen-Chung Lin**, Saratoga; **John D. Nguyen**, Milpitas, all of CA (US); **Roger A. Stoller**, Harwood Heights, IL (US); **Kristine N. Luong**, Santa Clara; **Robert S. Hudson**, San Jose, both of CA (US); **David A. Coleman**, Silverdale; **Dennis M. Sumners**, Port Orchard, both of WA (US); **Thanh T. Bui**, San Jose, CA (US); **Tony Fu**, Placentia, CA (US); **Tony G. Kwan**, Milpitas, CA (US)

(73) Assignee: **Adaptec, Inc.**, Milpitas, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/110,783**

(22) Filed: **Jul. 6, 1998**

Related U.S. Application Data

(60) Provisional application No. 60/075,687, filed on Feb. 24, 1998.

(51) **Int. Cl.**[7] **G06F 12/00**
(52) **U.S. Cl.** **711/162**; 717/11; 714/6
(58) **Field of Search** 711/162, 161; 717/11; 709/213; 713/2

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,269,022 * 12/1993 Shinjo et al. 713/2
5,469,573 * 11/1995 McGill, III et al. 717/11
5,694,600 * 12/1997 Khenson et al. 713/2
5,713,024 * 1/1998 Halladay 717/11
5,754,782 * 5/1998 Masada 709/213

OTHER PUBLICATIONS

Unknown, *"XactCopy"*, DuoCor, Inc., Nevada City, CA.

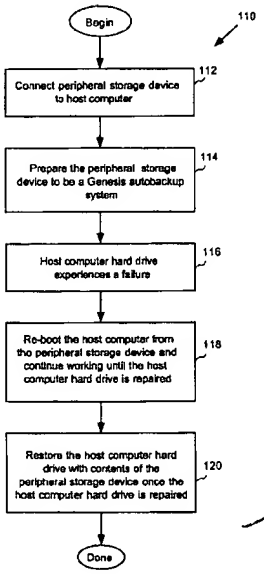
* cited by examiner

Primary Examiner—Do Yoo
Assistant Examiner—Nasser Moazzami
(74) *Attorney, Agent, or Firm*—Martine Penilla & Kim, LLP

(57) **ABSTRACT**

Disclosed is an apparatus, a system, a computer readable media, and a method for protecting data of a computer system. The method includes: (a) connecting a peripheral storage device to the computer system; (b) preparing a storage media of the peripheral storage device to be a protection enabled media; (c) selecting a backup set of data stored in a hard drive of the computer system, the backup set of data includes a default set of boot files and operating system files; (d) creating a spare tire backup using file-based copying from the hard drive of the computer system to the storage media of the peripheral storage device; (e) enabling the peripheral storage device to incrementally copy portions of the backup set of data from the hard drive of the computer system during normal use; and (f) booting the computer system from the peripheral storage device when a failure occurs with the hard drive that disables normal booting. In this manner, the user can resume uninterrupted work from the spare tire backup of the peripheral storage device until the hard drive failure is repaired.

35 Claims, 21 Drawing Sheets



related to other two ADAPTEC references herein included

used by the microprocessor **816** as a general storage area and as scratch-pad memory, and can also be used to store input data and processed data. The ROM **822** can be used to store instructions or program code followed by the microprocessor **816** as well as other data.

The peripheral bus **824** is used to access the input, output, and storage devices used by the digital computer **802**. In the described embodiment, these devices include the display screen **804**, the printer device **806**, the floppy disk drive **808**, the hard disk drive **810**, and the network interface **812**. The keyboard controller **826** is used to receive input from keyboard **814** and send decoded symbols for each pressed key to microprocessor **816** over bus **828**.

The display screen **804** is an output device that displays images of data provided by the microprocessor **816** via the peripheral bus **824** or provided by other components in the computer system **800**. The printer device **806** when operating as a printer provides an image on a sheet of paper or a similar surface. Other output devices such as a plotter, typesetter, etc. can be used in place of, or in addition to, the printer device **806**.

The floppy disk drive **808** and the hard disk drive **810** can be used to store various types of data. The floppy disk drive **808** facilitates transporting such data to other computer systems, and hard disk drive **810** permits fast access to large amounts of stored data.

The microprocessor **816** together with an operating system operate to execute computer code and produce and use data. The computer code and data may reside on the RAM **820**, the ROM **822**, or the hard disk drive **810**. The computer code and data could also reside on a removable program medium and loaded or installed onto the computer system **800** when needed. Removable program mediums include, for example, CD-ROM, PC-CARD, floppy disk and magnetic tape.

The network interface **812** is used to send and receive data over a network connected to other computer systems. An interface card or similar device and appropriate software implemented by the microprocessor **816** can be used to connect the computer system **800** to an existing network and transfer data according to standard protocols.

The keyboard **814** is used by a user to input commands and other instructions to the computer system **800**. Other types of user input devices can also be used in conjunction with the present invention. For example, pointing devices such as a computer mouse, a track ball, a stylus, or a tablet can be used to manipulate a pointer on a screen of a general-purpose computer.

The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can be thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, magnetic tape, optical data storage devices. The computer readable medium can also be distributed over a network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For example, although a preferred type of peripheral storage device is a Jaz™ drive, any type of peripheral storage devices or computer built-in storage devices can be used. In addition, the storage devices can either be physically located next to the computer system itself, or be remotely networked either over a local area network (LAN) or over the Internet.

In some embodiments, exemplary peripheral-type storage devices may include an extra hard drive(s), a digital video disk (DVD) drive, a CDRW drive, a CDR drive, a Magneto Optical Disk drive, etc. Furthermore, any type of host adapter can be used, whether it is integrated into a computer's mother board or is integrated onto a host adapter card. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

What is claimed is:

1. A method for protecting data of a computer system, comprising:

connecting a peripheral storage device to the computer system;

preparing a storage media of the peripheral storage device to be a protection enabled media, the preparing including,

writing one or more identification codes onto a first track of the storage media following a master boot record sector;

obtaining a serial number of the storage media; and

writing the one or more identification codes along with the obtained serial number into a registry file of the computer system;

selecting a backup set of data stored in a hard drive of the computer system, the backup set of data including a default set of boot files and operating system files;

creating a spare tire by copying the backup set of data from the hard drive of the computer system to the storage media of the peripheral storage device using a file-based copying scheme;

enabling the peripheral storage device to incrementally copy portions of the backup set of data from the hard drive of the computer system during normal use after creating the spare tire;

determining whether a failure occurs with the hard drive that disables booting to the hard drive; and

booting the computer system from the peripheral storage device using the spare tire.

2. A method for protecting data of a computer system as recited in claim **1**, wherein the preparing of the storage media of the peripheral storage device to be a protection enabled media further comprises:

re-formatting the storage media of the peripheral storage device;

partitioning the re-formatted storage media to one or more logical local partitions to match a partitioning scheme of the hard drive of the computer system; and

formatting each of the logical local partitions to match a formatting scheme of the hard drive of the computer system.

3. A method for protecting data of a computer system as recited in claim **1**, wherein the selecting of the backup set of data further comprises:

examining the hard drive of the computer system to identify programs and files that are stored on the hard drive, the programs and files being in addition to the default set of boot files and operating system files;

generating a user interface displaying the default set of boot files, operating system files, and the identified programs and files that are stored on the hard drive; and

selecting all of the identified programs and files if the storage media is sufficiently larger than a size of the default set of boot files, operating system files, and the

identified programs and files that are stored on the hard drive of the computer system, otherwise only selecting certain ones of the identified programs and files that are stored on the hard drive.

4. A method for protecting data of a computer system as recited in claim 3, wherein the selecting of the backup set of data further comprises:

generating a database file of the backup set of data, the database file being a pointer list identifying a location of each of the default set of boot files, operating system files, and selected programs and files stored on the hard drive of the computer system.

5. A method for protecting data of a computer system as recited in claim 1, further comprising:

scheduling when to incrementally copy portions of the backup set of data.

6. A method for protecting data of a computer system as recited in claim 5, further comprising:

collecting an e-mail address of a computer support personnel, and

sending an automatic e-mail message to the computer support personnel at the e-mail address after the failure occurs with the hard drive that disables booting to the hard drive.

7. A method for protecting data of a computer system as recited in claim 5, further comprising:

taking a footprint image of data stored on the hard drive of the computer system, the footprint image containing a list of operating system data, a list of peripheral device data, a list of controller card data, and a time stamp of when the footprint image was created.

8. A method for protecting data of a computer system as recited in claim 7, wherein the footprint image is written to a file in text format each time a successful boot to the hard drive of the computer system occurs.

9. A method for protecting data of a computer system as recited in claim 8, further comprising:

generating an after footprint image after the failure occurs with the hard drive that disabled booting to the hard drive;

comparing the after footprint image and the footprint image that is created each time the successful boot to the hard drive of the computer system occurs; and

generating information about a possible cause of the failure that disabled booting to the hard drive of the computer system.

10. A method for protecting data of a computer system as recited in claim 1, further comprising:

launching the spare tire;

determining whether booting to the peripheral storage device is desired to continue working in an uninterrupted state.

11. A method for protecting data of a computer system as recited in claim 10, further comprising:

suggesting a possible fix to the failure that disabled booting to the hard drive of the computer system; and

launching a repair suite to fix the failure.

12. A method for protecting data of a computer system as recited in claim 1, further comprising:

repairing the failure of the hard drive; and

restoring the hard drive of the computer system with the contents of the storage media of the peripheral storage device.

13. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system, the computer system having a peripheral storage device connected thereto, the system comprising;

a removable storage media that is configured to be placed into the peripheral storage device, the removable storage media being formatted to be a protection enabled media and containing a backup set of data including a default set of boot files and operating system files, the backup set of data being substantially continuously backed up on a schedule;

a spare tire launcher configured to be launched when the failure with the storage media of the user's computer system occurs to enable the user to re-boot to the peripheral storage device which contains a selected duplicate image of contents of the storage media of the user's computer system;

a preparation engine, the preparation engine being configured to perform the operations that comprise:

re-formatting the removable storage media of the peripheral storage device;

partitioning the re-formatted removable storage media to one or more logical local partitions to match a partitioning scheme of the storage media of the user's computer system;

formatting each of the logical local partitions to match a formatting scheme of the storage media of the user's computer system;

writing one or more identification codes onto a first track of the removable storage media following a master boot record sector;

obtaining a serial number of the removable storage media; and

writing the one or more identification codes along with the obtained serial number into a registry file of the user's computer system.

14. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim 13, wherein the system for protecting a user's productivity further comprises a foot print engine, the foot print engine being configured to perform the operations that comprise:

taking a footprint image of data stored on the storage device of the user's computer system, the footprint image containing a list of operating system data, a list of peripheral device data, a list of controller card data, and a time stamp of when the footprint image was created.

15. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim 14, wherein the footprint image is written to a file in text format each time a successful boot to the storage device of the user's computer system occurs.

16. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim 15, wherein the foot print engine is further configured to perform the operations that comprise:

generating an after footprint image when the failure occurs with the storage media that disables booting to the storage media;

comparing the after footprint image and the footprint image that is created each time the successful boot to the storage media of the user's computer system occurs; and

generating information about a possible cause of the failure that disabled booting to the storage media of the user's computer system.

17. A system for protecting a user's productivity upon detecting a failure with storage media of the user's computer system as recited in claim 13, wherein the backup set of data is copied from the storage media of the user's computer system to the removable storage media using a file-based copying scheme.

18. A computer readable media containing program instructions for protecting data of a computer system that has a peripheral storage device connected thereto, the computer readable media comprising:

program instructions for causing preparation of a storage media of the peripheral storage device to be a protection enabled media, the preparation including writing one or more identification codes onto a first track of the storage media following a master boot record sector, obtaining a serial number of the storage media, and writing the one or more identification codes along with the obtained serial number into a registry file of the computer system;

program instructions for enabling a selection of a backup set of data stored in a hard drive of the computer system, the backup set of data includes a default set of boot files and operating system files;

program instructions for enabling a generation of a spare tire backup that includes the backup set of data to the storage media of the peripheral storage device;

program instructions for enabling the peripheral storage device to incrementally copy portions of the backup set of data from the hard drive of the computer system during normal use; and

program instructions that enable booting the computer system from the peripheral storage device when a failure occurs with the hard drive that disables booting to the hard drive.

19. A computer readable media as recited in claim 18, wherein the program instructions for preparing the storage media of the peripheral storage device to be a protection enabled media further comprises:

program instructions for enabling of a re-formatting the storage media of the peripheral storage device;

program instructions for enabling a partitioning of the re-formatted storage media to one or more logical local partitions to match a partitioning scheme of the hard drive of the computer system; and

program instructions for enabling a formatting of each of the logical local partitions to match a formatting scheme of the hard drive of the computer system.

20. A computer readable media as recited in claim 18, wherein the program instructions for selecting of the backup set of data further comprises:

program instructions for examining the hard drive of the computer system to identify programs and files that are stored on the hard drive, the programs and files are in addition to the default set of boot files and operating system files;

program instructions for generating a user interface displaying the default set of boot files, operating system files, and the identified programs and files that are stored on the hard drive; and

program instructions for selecting all of the identified programs and files if the storage media is sufficiently larger than a size of the default set of boot files, operating system files, and the identified programs and files that are stored on the hard drive of the computer system, otherwise only selecting certain ones of the identified programs and files that are stored on the hard drive.

21. A computer readable media as recited in claim 20, wherein the program instructions for selecting of the backup set of data further comprises:

program instructions for generating a database file of the backup set of data, the database file being a pointer list identifying a location of each of the default set of boot files, operating system files, and selected programs and files stored on the hard drive of the computer system.

22. A computer readable media as recited in claim 18, further comprising:

program instructions for scheduling when to incrementally copy portions of the backup set of data.

23. A computer readable media as recited in claim 18, further comprising:

program instructions for collecting an e-mail address of a computer support personnel, and

program instructions for sending an automatic e-mail message to the computer support personnel at the e-mail address after the failure occurs with the hard drive that disables booting to the hard drive.

24. A computer readable media as recited in claim 18, further comprising:

program instructions for taking a footprint image of data stored on the hard drive of the computer system, the footprint image containing a list of operating system data, a list of peripheral device data, a list of controller card data, and a time stamp of when the footprint image was created.

25. A system for protecting data stored in a primary hard disk drive of a computer system, comprising:

preparing a storage media of a secondary peripheral storage device to be a protection enabled media;

selecting a backup set of data stored in the primary hard disk drive of the computer system, the backup set of data includes a default set of boot files and operating system files;

creating a spare tire backup by performing a file-based copy operation of the backup set of data from the primary hard disk drive of the computer system to the storage media of the secondary peripheral storage device;

enabling the secondary peripheral storage device to incrementally copy portions of the backup set of data from the primary hard disk drive of the computer system during normal use;

booting the computer system from the secondary peripheral storage device when a failure occurs with the primary hard disk drive which is detected by a system BIOS of the computer system; and

taking a footprint image of data stored on the primary hard disk drive of the computer system, the footprint image containing a list of operating system data, a list of peripheral device data, a list of controller card data, and a time stamp of when the footprint image was created, the footprint image being written to a file in text format each time a successful boot to the primary hard disk drive of the computer system occurs.

26. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim 25, wherein the preparing the storage media of the secondary peripheral storage device to be a protection enabled media further comprises:

re-formatting the storage media of the secondary peripheral storage device;

partitioning the re-formatted storage media to one or more logical local partitions to match a partitioning scheme of the primary hard disk drive of the computer system; and

formatting each of the logical local partitions to match a formatting scheme of the primary hard disk drive of the computer system.

27. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim **25**, wherein the preparing the storage media of the secondary peripheral storage device to be a protection enabled media further comprises:

writing one or more identification codes onto a first track of the storage media following a master boot record sector;

obtaining a serial number of the storage media; and

writing the one or more identification codes along with the obtained serial number into a registry file of the computer system.

28. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim **25**, wherein the selecting of the backup set of data further comprises:

examining the primary hard disk drive of the computer system to identify programs and files that are stored on the primary hard disk drive, the programs and files are in addition to the default set of boot files and operating system files;

generating a user interface displaying the default set of boot files, operating system files, and the identified programs and files that are stored on the primary hard disk drive; and

selecting all of the identified programs and files if the storage media is sufficiently larger than a size of the default set of boot files, operating system files, and the identified programs and files that are stored on the primary hard disk drive of the computer system, otherwise only selecting certain ones of the identified programs and files that are stored on the primary hard disk drive.

29. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim **28**, wherein the selecting of the backup set of data further comprises:

generating a database file of the backup set of data, the database file being a pointer list identifying a location of each of the default set of boot files, operating system files, and selected programs and files stored on the primary hard disk drive of the computer system.

30. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim **25**, further comprising:

scheduling when to incrementally copy portions of the backup set of data.

31. A system for protecting data stored in a primary hard disk drive of a computer system as recited in claim **25**, further comprising:

collecting an e-mail address of a computer support personnel, and sending an automatic e-mail message to the computer support personnel at the e-mail address after the failure occurs with the primary hard disk drive that disables booting to the primary hard disk drive.

32. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system, the system comprising;

a peripheral storage device having a storage media that is formatted to be a protection enabled media and contains a backup set of data including a default set of boot files and operating system files, the backup set of data being substantially continuously backed up on a schedule;

a host adapter basic input/output operating system (BIOS) being configured to receive an indication from a system BIOS that the failure has occurred with the storage media of the user's computer system, the host adapter BIOS being further configured to provide an option of re-booting the user's computer system from the peripheral storage device;

a computer user interface for providing options of repairing the storage media, restoring the storage media, or continue working from the peripheral storage device until the storage media is repaired and restored; and

a preparation engine that is configured to write one or more identification codes onto a first track of the storage media of the peripheral storage device following a master boot record sector, obtain a serial number from the storage media of the peripheral storage device, and write the one or more identification codes along with the obtained serial number into a registry file of the user's computer system.

33. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim **32**, further comprising:

a help notification system that is configured to automatically send an e-mail message to selected computer support, the e-mail message contains information that approximates a problem that caused the failure of the storage media.

34. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim **32**, wherein the host adapter BIOS is integrated on a small computer system interface (SCSI) host adapter controller that couples the computer system to the peripheral storage device.

35. A system for protecting a user's productivity upon detecting a failure with a storage media of the user's computer system as recited in claim **32**, wherein the preparation engine is configured to re-format the storage media of the peripheral storage device and partitioning the re-formatted storage media to one or more logical local partitions to match a partitioning scheme of the storage media of the user's computer system; and

wherein the formatting of each of the logical local partitions is configured to match a formatting scheme of the media of the user's computer system.

* * * * *

altavista

Advanced Web Search

○ **Build a query with...**

all of these words:

this exact phrase:

any of these words:

and none of these words

FIND

◉ **Search with...**

this boolean expression

crosstor

Use terms such as AND, OF
More>>

SEARCH: ○ Worldwide ◉ USA **RESULTS IN:** ◉ All languages ○ English, Spanish

Date:

○ by timeframe: Anytime

◉ by date range: 1 January 1980

1 January 2000

File type: Any format

Location

◉ by domain:

○ By URL:

Display:

☐ site collapse (on/off) What is this?

10 results per page

FIND

Clear Settings

White Paper

NETWORK-ATTACHED STORAGE (NAS) and STORAGE AREA NETWORKING (SAN)

May 1999

As storage capacity continues to grow at a compounded annual growth rate that exceeds 60%-90% for Windows NT-demands for external storage under centralized management persist. With these growing needs, continuous availability, ease of management, scalability, and resource sharing-ultimately in a heterogeneous environment-also receive increased emphasis. Two specific architectures are prime candidates to fulfill these requirements: Storage Area Networking (SAN) and Network Attached Storage (NAS).

Neither SAN nor NAS concepts are new, but their evpolution into the open system environments represents one of the most important changes affecting the storage industry in more than a decade. SAN and NAS are about to revolutionize the industry with ramifications extending beyond storage into network and systems management and architecture. SAN and NAS no longer couple storage directly to the server; this architectural change has important repercussions on the management of data in an enterprise.

This Paper covers NAS and compares NAS to SAN. Look for other Papers on SAN at http://www.periconcepts.com/

Network-attached storage (NAS)

Network-attached storage (NAS) is a fully integrated and dedicated storage solution. It can quickly and easily attach to a network topology, becoming immediately transparently available as a network resource for all clients. NAS is platform- and OS-independent, and appears to the application as another server. You can plug it in without shutting down the network, and it requires no changes to existing file servers.

NAS consists of a simplified server that performs only one function-and performs it well-not having to meet the conflicting requirements of a general-purpose OS. NAS can only run limited applications, but its ease-of-use and price/performance are unmatched. Implementations vary in which storage technologies and devices they support: Some may restrict themselves to CD-ROM, others to optical technologies, and still others may provide access to any storage technology including tape and magnetic disk.

NAS devices contain embedded processors running some sort of OS or microkernel that understands networking protocols and is optimized for I/O services. In contrast to the dedicated networks utilized with the storage area networking (SAN) architecture , NAS devices

directly attach to the standard messaging network, and are addressable via standard file-system protocols-for example, Network File System (NFS) or Common Internet File System (CIFS). These devices are typically optimized for particular tasks, such as file serving, and tend to accomplish these tasks at very high performance levels.

To applications running on the network, NAS looks like an ordinary server. To any client, it looks like a large storage device. If the NAS does little more than allow the network connection, it is called network-ready storage or a thin server. When NAS provides additional processing power to perform file and storage management tasks, it is called a network-attached storage server (NASS). NASS provides autonomy from a central server or CPU and optimizes the cost/performance ratio for a wide range of products covering multiple applications. It consolidates the storage of many application servers into a single storage service offered by one manageable pool of physical storage (Figure 1).

NASS may address the interoperability issue among different major platforms. Interoperability is an important feature that helps facilitate server consolidation in today's diverse operating environment. NASS usually takes advantage of NFS, CIFS, and NetWare Core Protocol (NCP) to be operational under different UNIX, Windows, and Novell NetWare platforms while providing simultaneous access to the same files from different platforms. The downside is that NASS systems move a great deal of data across the messaging network, potentially degrading overall network performance.

Major participants in the NAS market include Creative Design (CDS), Meridian, and Axis Communications at the low end; Network Appliance (NetApp), Unisys, LSI, Procom, and Artecon in the mid-range; and EMC and Auspex at the high end. Hewlett-Packard (HP) offers NAS jukebox solutions. Some software vendors offer a complete OS for NAS that can turn any hardware storage system into a multiprotocol file server for both UNIX and Windows clients. CrosStor is one of the leading vendors in this market.

A More Elegant Solution

Traditionally, the approach to solving network storage problems has been to add new drives and more processing power to available general-purpose/application servers or to add a new server. This approach does little to address the real problems of degraded response time, increased complexity, and availability of data. The advantages of NAS over conventional server-attached (or bus-attached) storage are performance and connectivity (see Figure 2). In addition, if you need an additional server to handle the new storage, a NAS solution is simpler and cheaper. NAS can produce improved file-access performance at a substantially lower cost than a general-purpose network server can. When factoring in the additional cost savings generated with a simple installation process, which literally takes minutes instead of hours or days, and ongoing reduced management costs, NAS is a better, more elegant solution.

New applications have created new requirements for high-speed transfer of very large files. General-purpose servers and most OSs were developed for fast processing in multiuser, multitasking environments and are a poor match for handling large files at high speeds. Performance problems and traffic bottlenecks develop when one server transmits data to another, or more accurately, when one storage device attached to a server transmits data to another storage device connected to another server on the other side of the network. NAS is optimized to move the data to users efficiently without the overhead and complexity of general-purpose servers. The controller's ability to connect anywhere on the network lets you balance

network performance by placing the storage close to the users who need the data. This architecture is particularly effective when bridges, routers, or switches segment the network.

Both storage area networking (SAN) and network-attached storage (NAS) technologies involve externalizing storage from the server and adding flexibility to network storage. With SAN technology, storage devices reside on their own networks with all the flexibility and performance benefits associated with networking. NAS technology involves employing a networking interface on storage devices, making them fully active nodes on the existing network. Both technologies come with comparative benefits and drawbacks.

Pros and Cons

The advantages of SAN reside in its superior performance, reliability, and connectivity. SANs offer a high-bandwidth link capable of growing incrementally and are better suited to transferring very large blocks of data. By contrast, the bandwidth properties of the data network characterize NAS networks, which are suited to efficiently move data in moderate-size segments. SAN delivers data reliability in a predicted time, while LANs (and NAS) retransmit data when the network is congested or fails for any reason. SAN offers a very high level of connectivity via cascading hubs and switches.

NAS devices typically see storage as files; SANs usually see blocks of data (see Table 1). This difference represents one of the major advantages of NAS configurations. Its other big advantages are ease-of-installation and its ability to offer low-cost entry product configurations. NAS doesn't require any significant initial investment, and the technology is available and proven.

NAS is not always a good idea for database applications because it's file-oriented. It works well, however, for document management and knowledge management applications. Because NAS does nothing but hold files for the network, it is flexible; however, it can also be inefficient at peak times due to network slowdowns. NAS devices work well for workgroups with high storage demands and in clustered server environments.

Each architecture has advantages depending on the application and existing infrastructure. The advantages of NAS include leveraging the current networking infrastructure and the enormous amount of development invested in this industry. NAS has a lead over SAN in heterogeneous data-sharing environments. SANs are at least two years away from offering this feature on a widespread commercial basis.

SANs and NAS are likely to coexist for some time and are, in many respects, complementary technologies. It appears likely that NAS functions will eventually migrate to the SAN. One way to think of NAS is as an important evolutionary step on the path to SAN.

By: Farid Neema

PERIPHERAL CONCEPTS, INC.
351 Hitchcock Way, Suite #B-200
Santa Barbara, California, 93105
Tel: (805) 563-9491
fneema@silcom.com

This article was published in the May 1999 issue of Windows NT Magazine

CROSSTOR SOFTWARE - Booth #F3
Sue Smith
4041 Hadley Road
South Plainfield, NJ 07080
Tel: 908-226-0100
FAX: 908-226-9596
E-mail:
Website: http://www.crosstor.com

COMPANY BACKGROUND:

CrosStor provides NAS, SAN and storage management software to OEMs. CrosStor software increases the reliability, availability, performance, and functionality of storage by making storage fundamentally more intelligent, easier to use and more manageable. An integrated, stackable architecture supports portable frameworks that operate across enterprise platforms and on the CrosStor NAS storage operating system. These frameworks export APIs that OEMs can use to easily create customized storage applications or, optionally, integrate with CrosStor-developed software. CrosStor's architectural modularity allows rapid integration, accelerates time to market and permits OEMs to focus internal resources on developing strategic, value-added software and storage system differentiation.

CrosStor is privately held and is headquartered in South Plainfield, New Jersey. The company has a software development division and Midwestern sales office in Colorado Springs, Colorado and a West Coast sales office in Fremont, California.

STORAGE NETWORKING PRODUCTS:

For storage appliance OEMs, CrosStor NAS is a multi-protocol, appliance operating system that includes CrosStor's programmable and flexible StackOS thin operating systems and the CrosStor FS high-availability, journaling file system. CrosStor NAS also includes CIFS, NFS and HTTP protocols and allows OEMs to create a single appliance that supports Microsoft Windows and UNIX files and provides unified directory services.

Going forward, CrosStor is pioneering standards that enhance existing NAS protocols to eliminate the distinctions among NAS, SAN and WAN - allowing all three types of hardware platforms to be integrated and administered as one. OEMs can work with CrosStor to create intelligent solutions for heterogeneous file sharing over SAN-based networks. With CrosStor SAN, OEMs can create unified NAS and SAN products that incorporate their associated security and naming models and are both based on the open file-sharing protocols.

Other CrosStor storage modules are: CrosStor Volume Manager - for software RAID and disk concatenation, CrosStor DMAPI - for hierarchical storage management, CrosStor SnapShot - for online backup, and CrosStor Remote Server Mirroring. CorsStor storage management modules integrate with CrosStor NAS and across open system platforms.

```
Set     Items   Description
S1    6867428   PLURAL? OR SEVERAL? OR MULTIPL? OR MULTIT? OR NUMEROUS? OR
            MANY OR MORE(2W)TWO
S2    5725278   THREE? OR TRIO? OR TRIUNE? OR TRIAD? OR TRIPL? OR TERTIAR?
            OR THIRD OR 3RD
S3    9122575   FIRST? OR 1ST OR PRIMARY OR INITIAL? OR ORIGINAL? OR LEADO-
            FF? OR MAIN OR CHIEF OR INTRODUCTORY?
S4    7469535   SECOND? OR 2ND OR DOUBL? OR TWIN? OR EXTRA? OR DUPLICAT? OR
             ANOTHER OR SUBSIDIAR? OR AUXILIAR?
S5      35279   BACK?()UP OR BACKUP?
S6     129991   REDUNDAN? OR FAILSAFE? OR FAIL()SAFE?
S7    2640188   RESERVE? OR SUPPLEMENTAL? OR SUPPLEMENTARY? OR EMERGENCY? -
            OR SUBSTITUT? OR SURROGAT?
S8    3618517   STORAG? OR STORE? OR STORING? OR MEMOR? OR CACHE? OR BUFFE-
            R? OR DOMAIN?
S9     204030   USER()INTERFACE? OR UI OR UIS OR GUI? ? OR (GRAPHIC? OR VI-
            SUAL?)(2W)INTERFACE?
S10     84557   MENU? ? OR DROPDOWN? OR DROP()DOWN? OR API? ? OR (APP OR A-
            PPS OR APPLICATION?)(2N)INTERFACE?
S11   1525483   EXCLUD? OR PREVENT?
S12   2106773   RESTRICT? OR DENY? OR DENIE? OR DENIAL? OR OBSTRUCT? OR BL-
            OCK? OR SHUTDOWN? OR SHUT?()DOWN
S13    512153   "NOT"()(ALLOW? OR ENABL? OR PERMIT?) OR DISALLOW? OR DISAB-
            L? OR SUSPEND? OR SUSPENSION?
S14    158253   AUTODISABL? OR NOGO OR NO()GO OR OFFSTATE? OR OFF()STATE? -
            OR INTERRUPT? OR TURNOFF? OR (TURN? OR SWITCH?)()OFF
S15    858103   STOP??? OR ARREST? OR IMPED? OR FORBID? OR HALT??? OR ABOR-
            T? OR SCRUB???? OR SCRATCH? OR NIX OR NIXES OR NIXED OR NIXING
S16       868   S1:S4 AND S5:S7 AND S8 AND S9:S10
S17       216   S16 AND S2
S18       106   S16 AND S11:S15
S19       284   S17:S18
S20        38   S17 AND S18
S21        21   S20 AND PY<2000
S22        19   RD  (unique items)
S23       246   S19 NOT S20
S24        99   S23 AND PY<2000
S25        96   RD  (unique items)
File   2:INSPEC 1898-2005/Nov W4
         (c) 2005 Institution of Electrical Engineers
File   6:NTIS 1964-2005/Nov W4
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2005/Nov W4
         (c) 2005 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Nov W4
         (c) 2005 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2005/Nov
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Dec W1
         (c) 2005 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2005/Oct W1
         (c)2005 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Oct
         (c) 2005 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Dec 06
         (c) 2005 The Gale Group
File 144:Pascal 1973-2005/Nov W4
         (c) 2005 INIST/CNRS
File 239:Mathsci 1940-2005/Jan
         (c) 2005 American Mathematical Society
```

25/3,K/95 (Item 8 from file: 256)
DIALOG(R)File 256:TecInfoSource

00118102 DOCUMENT TYPE: Review

PRODUCT NAMES: Omni-ISV (764451)

TITLE: New software lets ISVs link their storage **environments**
AUTHOR: Lelii, Sonia R
SOURCE: PC Week, v16 n29 p81(1) Jul 19, 1999
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 20031130

TITLE: New software lets ISVs link their storage **environments**

With CrosStor Software's Omni-ISV plan, independent software vendors (ISVs) can link their **storage** requirements with CrosStor's network-connected **storage** OS. Moreover, a NAS OS extension code set should be available in 4Q99 that will allow products from **third** -party providers to run in **storage** area networks (SANs). NAS appliances, which are easy to install **storage** devices that plug into networks, provide servers with easy access to data. SANs are groups of **storage** devices linked to a high-speed network that remains separate from the server network or...

...run in both NAS and SAN configurations; however, the Omni-ISV program will make available **application** programming **interfaces** (**APIs**) to CommVault Systems, for instance, to allow the **backup** /recovery software developer to run its software on both NAS and SAN devices. A spokesperson ...

DESCRIPTORS: Integration Software; LANs; Network Servers; Network Software ; Network Utilities; **Storage** Management; System Managed **Storage**
1999